CLAIMS:

What is claimed is:

1- In a System, a method for identifying devices and controlling the access of users and devices to information-related services based on the creation of a DIGITAL SIGNATURE for each requesting device, with no need for the use of biometrics or other security devices (i.e. smart cards), comprising the acts of:

Collecting data from devices by the execution of a Software Agent for the generation of a DIGITAL SIGNATURE where the Software Agent may be part of the original process of accessing a SERVICE;

The Software Agent processes data related to the software and hardware configurations collected from the Device and generates the DIGITAL SIGNATURE by using hashes which change at every access, and;

Sending an irreversible DIGITAL SIGNATURE of the device using several layers of cryptography to an Authentication Server.

2- The method of claim 1, characterized by the fact that the creation and sending of a DIGITAL SIGNATURE is one in several stages of a framework of authorization and authentication processes which aim to allow (or deny) the device to access the SERVICES, in which:

3- the method of claim 1, wherein an Authentication Server is accessed, receives and verifies the DIGITAL SIGNATURE, comparing same to previously stored DIGITAL SIGNATURES;

4- the method of claim 3, wherein the Authentication Server is capable of, based on configurations set by users or SERVICE providers, performing the acts of:

a) Identifying whether the device has been excluded from enrolling to or access to the SERVICE by means of a blacklist;

b) Creating a closed group of devices allowed to access the SERVICES, denying access to the SERVICES from any other device;

c) Creating a closed group of devices, denying the enrollment of additional devices to same;

d) Allowing a maximum number of enrollments for a particular device wherein the situation described in "a" above corresponds to a maximum number equal to zero;

e) remove a device from the enrolled devices list;

f) enroll additional devices.

5- the method of claim 3, wherein the Authentication Server is capable of, irrespective of configuration changes set by users or SERVICE providers, performing the acts of:

a) Allowing minor modifications to the software or hardware configurations of a previously enrolled device in a way as to (i.) maintain access to SERVICE for validly enrolled devices, and; (ii.) maintain recognition of devices included in blacklists, denying same access to the SERVICE;

b) Updating the DIGITAL SIGNATURES for devices in the situation described in the previous item once access to the SERVICE has been granted;

c) Submitting any enrolled device which has undergone major modifications to its hardware of software configurations to the same treatment as not-enrolled devices;

d) Logging all accesses or attempted accesses of a device to a SERVICE, maintaining said logs even if the device is removed or unregistered;

e) Denying a user the right to unregister, from a device lower in the registration hierarchy (i.e. a device registered or enrolled at a later time), a device higher in the registration hierarchy (i.e. a device registered or enrolled at an earlier time);

f) Denying a user the right to deactivate the Invention from a device lower in the registration hierarchy (i.e. a device registered or enrolled at a later time).

6- the method of claim 1, where a previously identified user, with no enrolled devices, accesses the Invention for the first time, comprising the acts of:

a) the SOFTWARE AGENT generates a DIGITAL SIGNATURE as described in claim 1;

b) the AUTHENTICATION SERVER verifies the parameter listed in claim 4 a;

c) the AUTHENTICATION SERVER verifies the parameter listed in claim 4 c and 4 d ;

d) based on user confirmation, the DIGITAL SIGNATURE is registered, the device is included in the authorized group and user is granted access to the SERVICE;

b) if item "b" above is not met, access to the SERVICE is denied;

7- the method of claim 1, where a previously identified user accesses the Invention from a registered device, comprising the acts of:

a) the SOFTWARE AGENT generates a DIGITAL SIGNATURE for the device;

b) the AUTHENTICATION SERVER recognizes the DIGITAL SIGNATURE and authorizes access to the SERVICE if successful.

8- the method of claim 1, where a previously identified user accesses the Invention from an unregistered device, comprising the acts of:

a) the SOFTWARE AGENT generates a DIGITAL SIGNATURE for the device;

b) the AUTHENTICATION SERVER verifies the parameters listed in claims 4 a and 4 b, and,

c) the AUTHENTICATION SERVER follows the steps described in claim 6, items "c" and "d";

d) if the requirement listed in item "b" above is not met, access to the SERVICE is denied.

5

9- In a System, the use of a method for identifying devices and controlling the access of users and devices to information-related services based on the creation of a DIGITAL SIGNATURE for each requesting device, with no need for the use of biometrics or other security devices (i.e. smart cards), in the method described in claims 1 thru 8, comprising the acts of:

Collecting data from devices by the execution of a Software Agent for the generation of a DIGITAL SIGNATURE where the Software Agent may be part of the original process of accessing a SERVICE;

The Software Agent processes data related to the software and hardware configurations collected from the Device and generates the DIGITAL SIGNATURE by using hashes which change at every access, and;

Sending an irreversible DIGITAL SIGNATURE of the device using several layers of cryptography to an Authentication Server.

10- The method of claim 9, characterized by the fact that the creation and sending of a DIGITAL SIGNATURE is one in several stages of a framework of authorization and authentication processes which aim to allow (or deny) the device to access the SERVICES, in which:

11- the method of claim 9, wherein an Authentication Server is accessed, receives and verifies the DIGITAL SIGNATURE, comparing same to previously stored DIGITAL SIGNATURES;

12- the method of claim 11, wherein the Authentication Server is capable of, based on configurations set by users or SERVICE providers, performing the acts of:

a) Identifying whether the device has been excluded from enrolling to or access to the SERVICE by means of a blacklist;

b) Creating a closed group of devices allowed to access the SERVICES, denying access to the SERVICES from any other device;

c) Creating a closed group of devices, denying the enrollment of additional devices to same;

d) Allowing a maximum number of enrollments for a particular device wherein the situation described in "a" above corresponds to a maximum number equal to zero;

e) remove a device from the enrolled devices list;

f) enroll additional devices.

13- the method of claim 11, wherein the Authentication Server is capable of, irrespective of configuration changes set by users or SERVICE providers, performing the acts of:

a) Allowing minor modifications to the software or hardware configurations of a previously enrolled device in a way as to (i.) maintain access to SERVICE for validly enrolled devices, and; (ii.) maintain recognition of devices included in blacklists, denying same access to the SERVICE;

b) Updating the DIGITAL SIGNATURES for devices in the situation described in the previous item once access to the SERVICE has been granted;

c) Submitting any enrolled device which has undergone major modifications to its hardware of software configurations to the same treatment as not-enrolled devices;

d) Logging all accesses or attempted accesses of a device to a SERVICE, maintaining said logs even if the device is removed or unregistered;

e) Denying a user the right to unregister, from a device lower in the registration hierarchy (i.e. a device registered or enrolled at a later time), a device higher in the registration hierarchy (i.e. a device registered or enrolled at an earlier time);

f) Denying a user the right to deactivate the Invention from a device lower in the registration hierarchy (i.e. a device registered or enrolled at a later time).

14- the method of claim 9, where a previously identified user, with no enrolled devices, accesses the Invention for the first time, comprising the acts of:

a) the SOFTWARE AGENT generates a DIGITAL SIGNATURE as described in claim 9;

b) the AUTHENTICATION SERVER verifies the parameter listed in claim 12 a;

c) the AUTHENTICATION SERVER verifies the parameter listed in claim 12 c and 12 d ;

d) based on user confirmation, the DIGITAL SIGNATURE is registered, the device is included in the authorized group and user is granted access to the SERVICE;

b) if item "b" above is not met, access to the SERVICE is denied;

15- the method of claim 9, where a previously identified user accesses the Invention from a registered device, comprising the acts of:

a) the SOFTWARE AGENT generates a DIGITAL SIGNATURE for the device;

b) the AUTHENTICATION SERVER recognizes the DIGITAL SIGNATURE and authorizes access to the SERVICE if successful.

16- the method of claim 9, where a previously identified user accesses the Invention from an unregistered device, comprising the acts of:

a) the SOFTWARE AGENT generates a DIGITAL SIGNATURE for the device;

b) the AUTHENTICATION SERVER verifies the parameters listed in claims 12 a and 12 b, and,

c) the AUTHENTICATION SERVER follows the steps described in claim 14, items "c" and "d";

d) if the requirement listed in item "b" above is not met, access to the SERVICE is denied.